IDEOVÝ ZÁMER

Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok

Identifikácia projektu

Názov:	Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Ružomberok
Realizátor:	Mesto Ružomberok
Kontaktná osoba:	PhDr. Vladimíra Pazderová, PhD. vladimira.pazderova@novofunding.sk Ing. Martin Žabenský zabensky@ruzomberok.sk
Dátum:	21.6.2024
Predpokladaný začiatok:	01.01.2025
Dátum schválenia projektovou komisiou:	

1. POPIS PROJEKTU

1.1. STRUČNÝ POPIS VÝCHODISKOVEJ SITUÁCIE

Mesto Ružomberok, ktoré je v zmysle zákona č. 69/2018 Z. z. poskytovateľom základnej služby, stojí podobne ako ďalšie mestá v súčasnosti pred výzvami v oblasti kybernetickej a informačnej bezpečnosti (ďalej len "KIB"), ktoré vyplývajú z rýchleho rozvoja digitálnych technológií a neustáleho zvyšovania množstva citlivých dát, ktoré je potrebné ochraňovať. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj dopady bezpečnostných incidentov. V zmysle platnej legislatívy nastavujú požiadavky a štandard z pohľadu KIB práve zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe.

Mesto je prevádzkovateľom nasledovnej základnej služby:

- Správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Na prevádzke danej základnej služby sa podieľajú tieto systémy:

- Informačný systém mesta ISS Cora Geo
- Dokumentačný informačný systém samosprávy Cora Geo DISS
- Mail server
- Web server

Mesto má relatívne rozsiahlu heterogénnu infraštruktúru informačných systémov a aplikácií, prostredníctvom ktorých poskytuje služby verejnosti. Súčasne túto infraštruktúru využívajú tiež organizácie naviazané na mestský úrad. Vykonaním samohodnotenia v meste Ružomberok a zrealizovaním kybernetického auditu boli identifikované kritické hrozby s výrazným dopadom na fungovanie Mestského úradu Ružomberok:

- zamestnanci pri ukončení pracovného pomeru alebo iného obdobného pracovného vzťahu zadokumentovaným spôsobom nevracajú späť všetky zverené aktíva,
- identifikácia zraniteľnosti rizík je neaktualizovaná /posledná aktualizácia je z roku 2021/,
- identifikácia hrozieb sa nerobila, je zastaraná a nezodpovedá aktuálnemu zoznamu identifikovaných aktív,
- identifikácia a analýza rizík sa nerobila,
- dokumentácia KIB neobsahuje učeného vlastníka rizika,
- v meste nie sú zadefinované postupy pre presun práv a povinnosti k vzťahu ku kybernetickej bezpečnosti pre IT špecialistov a členov HT,
- PZS nemá vypracovaný plán vzdelávania, v rámci rozvoja bezpečnostného povedomia sa za posledné dva roky nekonalo žiadne školenie zamestnancov,
- nevykonáva sa kontrola dodržiavania bezpečnostných politík pre dodávateľov a zamestnancov,
- hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia sa za posledné dva roky nerobilo,
- nie sú vypracované postupy pri skončení pracovného pomeru,
- PZS má identifikované tretie strany a s nimi uzavreté zmluvy, voči tretím stranám neboli vykonávané riziká spojené s dodávateľskými službami,
- vyhodnocovanie prevádzkových záznamov sa nevykonáva,
- nevykonáva sa detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
- PZS nepoužíva nástroj na detegovanie zraniteľnosti technických prostriedkov a ich častí,
- PZS nemá zavedený proces riadenia záplat a aktualizácií,
- bezpečnostná segmentácia siete nie je vytvorená,

- SIEM nie je vybudovaný,
- PZS nepoužíva nástroj na detekciu kybernetických bezpečnostných incidentov,
- nie je implementovaný nástroj na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí,
- zatiaľ nebola spracovaná analýza finančných nákladov na spracovanie dokumentácie BCM, technických a personálnych zdrojov,
- chýba BIA a RPO,
- neboli zatiaľ spracované procesy riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby.

Úroveň služieb všetkých dotknutých subjektov priamo závisí od funkčnosti informačných systémov mesta a niektoré služby sú od ich schopnosti prevádzky dokonca plne závislé. Nedostupnosť informačných aktív v dôsledku kybernetického incidentu preto môže mať fatálny vplyv nielen na základnú službu a poskytovanie ostatných služieb mesta ale i jeho organizácií, ktoré sú na jeho infraštruktúru naviazané.

Z dôvodu zabezpečenia súladu s požiadavkami zákonov o kybernetickej bezpečnosti a informačných technológiách vo verejnej správe bolo mestom vykonané samohodnotenie a zrealizovaný audit. Táto analýza odhalila viaceré kritické oblasti ktoré bezprostredne alebo potenciálne ohrozujú poskytovanie základnej služby. Časť opatrení eliminujúcich bezpečnostné riziká súvisiace s prevádzkou informačných systémov mesta bola vykonaná. Vzhľadom na obmedzené zdroje (finančné, personálne) ale neboli realizované všetky, a preto je nevyhnutné realizovať ďalšie opatrenia, ktoré umožnia ďalšie zvýšenie bezpečnosti ich prevádzky. S ohľadom na uvedené sa ako najvýznamnejšie problémy čoraz viac prejavujú:

1. **Nedostatočné riadenie rizík a zraniteľností:** Mesto čelí bez jasného prehľadu o tom, kde presne je zraniteľné, riziku neefektívneho využívania zdrojov na ochranu aktív alebo k opomenutiu kritických hrozieb. V oblasti riadenia rizík chýbajú aktualizované informácie ktoré by efektívne preskúmali identifikované riziká v závislosti od prijatých bezpečnostných opatrení.
2. **Nedostatočné monitorovanie a detekcia hrozieb v reálnom čase:** Absencia komplexných systémov pre monitorovanie a reakciu na bezpečnostné incidenty v reálnom čase obmedzuje schopnosť efektívne reagovať na potenciálne hrozby.
3. **Problémy s kontinuitou činností pri krízových situáciách:** V prípade krízovej situácie ako kybernetického bezpečnostného útoku alebo vzniknutého incidentu neexistujú postupy pre obnovu napadnutých systémov. Nedostatočná príprava na tieto udalosti môže viesť k dlhodobému prerušeniu služieb a ťažko obnoviteľným finančným a operačným škodám.
4. **Zastaraná a nehomogénna sieťová infraštruktúra:** Mesto má staré a rôzne sieťové prvky, ktoré potrebujú výmenu a modernizáciu, vrátane zabezpečenia redundancie a zlepšenia sieťovej segmentácie.
5. **Zraniteľná serverová infraštruktúra:** Používanie zariadení, ktoré sú na konci svojej životnosti (EOL - End of Life), predstavuje bezpečnostné riziko a môže ohroziť dostupnosť poskytovaných služieb.
6. **Nedostatočný monitoring všetkých IT aktív:** môže viesť k prehliadnutiu anomálií, nesprávnemu fungovaniu systémov a oneskoreným reakciám na bezpečnostné incidenty. Absencia adekvátnych monitorovacích nástrojov a procesov znamená, že problémy môžu zostať neodhalené až do okamihu, keď spôsobia významné narušenie prevádzky alebo bezpečnosti.
7. **Nedostatočná zálohovacia stratégia a plány:** Absencia robustnej zálohovacej stratégie a plánov zvyšuje riziko straty dát v prípade zlyhania hardvéru alebo kybernetických útokov ako je napr. ransomware.
8. **Nedostatočná kontrola a monitorovanie sieťového obsahu:** Chýba pokročilé monitorovanie obsahu a tokov dát, čo môže viesť k únikom dát a bezpečnostným incidentom.
9. **Nedostatočná validácia efektivity zavedených bezpečnostných opatrení:** Potreba vykonať audit a penetračné testy na konci projektu s cieľom validovať účinnosť implementovaných bezpečnostných opatrení a identifikovať zostávajúce potrebné oblasti zlepšenia.

Práve s ohľadom na vyššie uvedené nedostatky je predmetom projektu súbor riešení, ktoré zlepšia celkovú úroveň kybernetickej bezpečnosti mesta a umožnia dosiahnuť požadovanú úroveň jeho KIB v súlade s platnou legislatívou.

Zámerom projektu je posilniť kybernetickú a informačnú bezpečnosť mesta Ružomberok prostredníctvom komplexného prístupu zameraného na zlepšenie viditeľnosti a kontroly nad informačnou infraštruktúrou. V rámci projektu sa budú realizovať nasledujúce kľúčové opatrenia:

1. **Aktualizácia analýzy rizík** zabezpečí správu aktív, zraniteľností, hrozieb a opatrení. Analýza rizík umožní aktualizovanie a hodnotenie rizík založené na aktuálnych dátach a poskytne nástroje pre efektívne riadenie a minimalizáciu rizík.
2. **Vybudovanie Security Incident and Event Management (SIEM):** Opatrenie je zamerané na vytvorenie nástroja zabezpečujúceho analýzu informácií zo všetkých sieťových zariadení, OS, databáz, aplikácií a pod., ktorými žiadateľ disponuje (SIEM), ktoré bude kompletne vybudované vo vlastníctve žiadateľa, tzv. on premise.
3. **Vypracovanie a implementácia komplexného plánu kontinuity činností (BCM),** ktorý zahŕňa postupy pre rýchlu obnovu kritických systémov a služieb po narušení. Plán bude obsahovať scenáre pre rôzne typy udalostí a zahrnie analýzu funkčných dopadov, strategické zdroje na obnovu a časové rámce pre reakciu.
4. **Modernizácia sieťovej infraštruktúry v mestskej informačnej sieti:** Zabezpečí sa výmena zastaraných sieťových prvkov, dobudovanie záložných trás a rozšírená segmentácia siete. Tieto kroky významne prispejú k zníženiu zraniteľností vyplývajúcich z používania EOL zariadení a ich nedostatočného zabezpečenia.
5. **Modernizácia serverovej infraštruktúry:** Výmena serverových komponentov, sieťových prvkov prispeje k zníženiu rizika nízkej dostupnosti poskytovania základnej služby a zraniteľnosti spojenej s používaním zastaraných zariadení.
6. **Zavedenie a správa nástroja na riadenie kapacít,** ktorý umožní nepretržité sledovanie všetkých IT aktív, poskytovanie včasných upozornení na potenciálne problémy a umožní rýchlu reakciu na incidenty. Týmto spôsobom sa zlepší viditeľnosť a kontrolu nad IT infraštruktúrou, čím sa zabezpečí jej spoľahlivú a bezpečnú prevádzku.
7. **Nastavenie zálohovania:** zavedenie stratégie a plánov zálohovania zabezpečí zvýšenie dostupnosti základnej služby.
8. **Implementácia next-gen firewall technológie:** Umožní pokročilé filtrovanie obsahu, riadenie prestupov medzi sieťovými segmentami a integráciu s aktuálnymi bezpečnostnými systémami. Táto technológia adresuje zraniteľnosti spojené s nedostatočnou kontrolou sieťového obsahu a potenciálnymi sieťovými útokmi na infraštruktúru
9. **Vykonanie auditu kybernetickej bezpečnosti:** Vykonanie auditov a penetračných testov na konci projektu poskytne hodnotné prehľady o efektívnosti prijatých opatrení a pomôže identifikovať ďalšie možnosti zlepšenia.

Implementáciou týchto technických opatrení v rámci celkového projektu kybernetickej a informačnej bezpečnosti sa zvýši odolnosť mesta proti kybernetickým hrozbám a zlepší sa ochrana dát a základnej služby.

Zvyšovanie úrovne v oblastiach procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia je nevyhnutné pre zvýšenie kapacít mesta v oblasti kybernetickej a informačnej bezpečnosti. To zahŕňa nielen aktualizáciu a posilnenie fyzickej a IT infraštruktúry, ale aj budovanie a rozvoj organizácie KIB v meste, aby bolo schopné plniť úlohy v tejto oblasti.

Cieľová skupina tohto projektu zahŕňa nielen zamestnancov mesta, ale aj občanov, ktorý sa spoliehajú na digitálne služby poskytované mestom.

Projekt si tiež kladie za cieľ podporiť včasnú detekciu kybernetických incidentov a zvýšiť schopnosť reakcie mesta na takéto hrozby. Je dôležité adaptovať najmodernejšie technológie a postupy, čím sa zvýši odolnosť základnej služby mesta proti kybernetickým hrozbám.

Vzhľadom na komplexnosť a dôležitosť tohto projektu je prioritou jeho včasná realizácia, aby sa predišlo potenciálnym rizikám a zabezpečila vysoká úroveň ochrany pre všetky zainteresované strany.

Realizácia vyššie navrhovaných opatrení umožní vytvoriť robustnejšiu infraštruktúru, ktorá bude funkčne a kapacitne vyhovovať potrebám nevyhnutným pre poskytovanie služieb mesta a z bezpečnostného hľadiska spĺňať legislatívne požiadavky. Zároveň umožní nastaviť procesy a postupy, ako tento stav v čase zachovať a rozvíjať v nadväznosti na požiadavky vyplývajúce zo zmeny legislatívy resp. rozsahu poskytovaných služieb.

1.2. SITUÁCIA PO REALIZÁCII PROJEKTU

Po úspešnej implementácii projektu sa predpokladá výrazné posilnenie kybernetickej a informačnej bezpečnosti. Tento projekt prináša komplexné vylepšenia v rôznych oblastiach, zaručujúc robustnejšiu ochranu pre infraštruktúru mesta a zvyšujúc odolnosť proti kybernetickým hrozbám.

V oblasti infraštruktúry dôjde k výraznému posilneniu prostredníctvom modernizácie sieťovej infraštruktúry, zlepšenia redundancie a zavedenia pokročilých monitorovacích a reakčných systémov. Tieto opatrenia zabezpečia rýchlejšie odhaľovanie a reagovanie na bezpečnostné incidenty, čo je kľúčové pre minimalizáciu rizík a potenciálnych škôd.

Modernizácia serverovej a sieťovej infraštruktúry posilní schopnosť mesta udržať nepretržitú dostupnosť kritických služieb a efektívne reagovať na incidenty súvisiace so stratou údajov.

Výsledkom realizácie projektu bude mesto Ružomberok, ktoré je nielen lepšie chránené pred kybernetickými hrozbami, ale je tiež pripravené na využívanie digitálnych príležitostí s väčšou dôverou a bezpečnosťou pre všetkých svojich obyvateľov.

1.3. ÚPRAVA PROCESOV

Vychádzajúc z výsledkov nedávneho auditu kybernetickej bezpečnosti, ktorý odhalil potrebné oblasti zlepšenia, sa mesto zameria na predbežné úpravy svojich procesov pred zavedením vybraných opatrení.

Prvým krokom bude dôkladná analýza a optimalizácia súčasných procesov, aby sa zabezpečilo, že nové technológie budú implementované efektívne a budú podporovať už existujúce zjednodušené postupy. Týmto sa zvýši celková úroveň kybernetickej a informačnej bezpečnosti v meste Ružomberok.

Následne sa mesto zameria na integráciu nových opatrení tak, aby sa prirodzene integrovali do upravených procesov. To bude zahŕňať aj aktualizáciu interných smerníc a príslušnej dokumentácie, čím sa zabezpečí súlad dokumentov s novými postupmi a technológiami. Tento prístup umožní hladkú integráciu a zvýši efektivitu nových riešení v rámci organizácie. Kľúčovou súčasťou bude aj zaškolenie zamestnancov, ktoré im poskytne potrebné znalosti a zručnosti pre prácu s novými nástrojmi a v rámci optimalizovaných procesov pre oblasť KIB. To zvýši ich schopnosť efektívne reagovať na bezpečnostné výzvy a prispieť k ochrane identifikovaných aktív mesta. Po komplexnej implementácii týchto opatrení, bude mesto Ružomberok lepšie vybavené na detekciu a reakciu na kybernetické hrozby, čo výrazne zvýši úroveň KIB v meste. Zvýšená kybernetická a informačná odolnosť tak prispeje k posilnenej dôvere v digitálne služby, ktoré mesto poskytuje svojim obyvateľom a návštevníkom.

2. POUŽÍVATELIA RIEŠENIA

Počas vykonaného auditu kybernetickej bezpečnosti sa aktívne získavali názory kľúčových používateľov, ktoré poskytli detailný pohľad na súčasný stav a identifikovali kritické oblasti potrebné pre zlepšenie. Tento proces odhalil, že používatelia vnímajú problémy súvisiace s ochranou dát, prístupnosťou k systémom a celkovou pripravenosťou na kybernetické hrozby. Aj na základe týchto informácií sa navrhli zlepšenia, ktoré sú obsahom projektu.

V rámci projektu budú kľúčoví používatelia zapojení do fázy testovania opatrení s cieľom zabezpečiť, aby konečné výsledky reflektovali ich potreby a zlepšili celkovú kybernetickú a informačnú bezpečnosť v meste. Okrem toho bude zabezpečené, že všetci používatelia budú adekvátne oboznámení a zaškolení na prácu s novými systémami a procesmi, čo zvýši ich efektivitu a prispeje k bezpečnejšiemu prostrediu mesta Ružomberok.

Týmto spôsobom sa mesto zaväzuje k tomu, že vývoj a implementácia nových bezpečnostných opatrení bude v súlade s potrebami a očakávaniami tých, ktorí ich budú najviac využívať, čo prispieva k vyššej úrovni spokojnosti a bezpečnosti pre všetkých.

3. PRÍNOSY

V rámci projektu zameraného na zvýšenie kybernetickej a informačnej bezpečnosti v meste sme identifikovali nasledovné prínosy, ktoré prinesie realizácia tohto projektu. Tieto prínosy sú spojené s konkrétnymi problémami, ktoré identifikoval audit v rámci aktuálneho stavu KIB v meste Ružomberok.

1) **Zvýšenie úrovne kybernetickej a informačnej bezpečnosti:** Implementáciou opatrení v rámci projektu bude očakávame zníženie počtu identifikovaných kritických rizík aj na základe vykonaného auditu a realizovanej analýzy rizík na konci projektu.
2) **Zníženie počtu bezpečnostných incidentov:** Vďaka posilnenej kybernetickej a informačnej bezpečnosti očakávame pokles počtu bezpečnostných incidentov v meste.
3) **Zlepšená spokojnosť a dôvera používateľov:** Implementácia projektu bude viesť k vyššej spokojnosti občanov a zamestnancov s digitálnymi službami mesta, čo zvyšuje ich dôveru v tieto služby.
4) **Posilnené povedomie o kybernetickej bezpečnosti:** V rámci rozvoja manažmentu KIB v meste bude zvýšené povedomie zamestnancov o dôležitosti kybernetickej bezpečnosti. Toto je kľúčové pre prevenciu a efektívnu reakciu na incidenty.

Prínosy projektu budú pravidelne monitorované a vyhodnocované počas jeho realizácie, aj počas obdobia udržateľnosti projektu, aby sa preukázalo, že ciele projektu sú dosiahnuté a prínosy sú trvalé a merateľné.